

Information Systems Security Rules for Service Providers (RSSIPS) at CDC

Internal



**Caisse
des Dépôts**
GROUPE



Contents

01.	Introduction	3
02.	Access to resources	7
03.	Proper use of resources	9
04.	Intellectual property	16
05.	Protection of information and personal data	18
06.	Controlling use of resources	20
07.	File servers	22
08.	Information note: personal data	24

01

Introduction

1.1

Purpose of the document

- The purpose of this document, hereinafter referred to as the "RSSIPS" (Règles de Sécurité des Systèmes d'Informations pour les Prestataires de Services / Information Systems Security Rules for Service Providers), is to explain the rules currently in force at CDC and is intended for service providers who are users, even if only occasionally, of CDC's IT resources made available to them strictly for the purposes of performing their services.
- These RSSIPS illustrate the respectful and responsible behaviour that everyone is obliged to adopt with regard to the resources made available to them.
- Consequently, the service provider, prior to any use of CDC's IT resources:
 - undertakes to apply these RSSIPS in the performance of the services entrusted to it;
 - undertakes to ensure compliance on the part of all its employees and any subcontractors involved in the performance of the services entrusted to it;
 - undertakes to keep and provide, if so requested by CDC, the original certificate signed by its employees and any subcontractors involved in performing the services entrusted to it, in accordance with the model appended to these RSSIPS.

1.2

Definitions

- By "resources", we mean any element involved in the implementation and operation of an information system (information in all its forms, individual equipment, printers, software, file servers, databases, applications, network equipment, internal/external network services, disk space, email, etc.).
- By "User", we mean any natural person who accesses and/or uses CDC's and its clients' resources, including the staff of CDC's service providers and their possible subcontractors.

1.3

Regulatory framework

- The resources made available by CDC and all the data they contain are the property of CDC and/or its clients.
- All users of these resources, including service providers' staff (and their subcontractors), must comply with the general security and confidentiality policies implemented by CDC, as well as with the rules of good conduct set out in this document, in accordance with current legislation and regulations.
- All users authorised by CDC to access its and/or its clients' information systems remain subject to general civil and criminal law in their use of resources. They are solely responsible for any use made of the resources from their account and their authorisations, and undertake not to use them for activities that are illicit and/or contrary to public order and common decency, and/or likely to be prejudicial to CDC, its clients or third parties, but to use them solely for the performance of services.
- Each CDC service provider undertakes to ensure that its staff and any subcontractors who may use CDC's and/or its clients' resources for the purposes of providing services expressly accept the rules set out in these RSSIPS.

02

Access to resources

- Access by a user to CDC's and/or its clients' resources is only possible for the purposes of performing the services defined in the service contract, and within the limits of the authorisations granted, which may be modified or withdrawn by CDC.
- Access to resources is subject to authentication (a unique identifier coupled with a unique authenticator, which can be a password) and associated with authorisations that must be limited. Accessing a resource is an identified personal responsibility, with rights and duties for proper control of logical access to the CDC's IS.
- Authentication means are personal, confidential and non-transferable. Consequently, uses made with the help of a means of authentication specific to each user are deemed to have been made by the holder of such means of authentication, unless proven otherwise.
- *The user must not circumvent the access security devices in place or access, or attempt to access, resources for which they are not authorised.*

03

Proper use of resources

3.1

General proper use of resources

- The user is responsible for the use they make of the resources made available to them for the purposes of performing their services. This principle of responsibility implies appropriate behaviour.
- In particular, the user must not:
 - Make CDC's and/or its clients' resources available to unauthorised persons, whether internal or external to CDC;
 - Attempt to read, modify, copy or destroy information other than that which belongs to them or for which they have corresponding rights;
 - Circumvent restrictions on use of resources made available by CDC;
 - In particular, circumvent *Data Leak Prevention* (DLP) systems or any control or monitoring system set up by CDC in order to ensure the security of its information systems and of which the user has been duly informed;
 - Copy or process information and/or data belonging to CDC and/or its clients on individual equipment not owned by CDC and without CDC's express prior authorisation; Fraudulently access, break into, maintain and/or alter elements contained in the CDC's and/or its clients' IS and/or prevent its operation, or make any attempt to do so.
- In particular, the following will be considered abusive within the meaning of the RSSIPS: behaviour aimed at organising reception of, consulting or attempting to consult, downloading, storing, publishing, broadcasting or distributing, knowingly, by means of CDC resources, any programs, software, electronic documents, messages, information or data:
 - Aiming to denigrate CDC and/or its clients, and damaging its brand image, interests or reputation;
 - Violent, paedopornographic, pornographic, xenophobic, revisionist, negationist, racist or sectarianist in nature, and, more generally, contrary to the regulations in force;
 - Likely to undermine respect for the individual, their dignity or privacy;

- Defamatory in nature;
 - Aiming to harass, threaten or insult;
 - Containing elements protected by the laws on intellectual property and image rights, unless the necessary authorisations have been obtained;
 - Inciting commission of a misdemeanour or felony or, in general, actions that are illegal or contrary to public order;
 - Contrary to common decency;
 - Bearing on CDC's or its clients' information, in breach of their obligation of confidentiality.
- *Users must be vigilant in order to avoid unintentional incidents and detect malicious acts targeting resources.*
- *Users must comply with the classification of information according to its level of confidentiality: a document is considered confidential when its public dissemination could be detrimental to CDC and/or its partners and clients (a financial loss, disruption of a department's operation, infringement of such legislation as the GDPR, a possible labour dispute, loss of markets or investment, or an unfavourable article in the media). Use of CDC's information and documents must not go beyond the scope of CDC's activities.*

3.2

Use of mobile computing devices

- It should be noted that any mobile equipment made available to users by CDC on an exceptional basis is CDC's property and is only intended for use in the context of performance of their services.
- Nomadism requires rigorous vigilance in order to avoid any loss and/or theft of CDC's equipment and the information and data stored on it.

3.3

Uses of email

- Use of email by the user is only authorised in the context of performance of their services. The email user is clearly identified as a CDC service provider.
- Certain specific rules must be complied with, in particular:
 - The content of electronic messages is confidential;
 - Rerouting messages to an email address external to CDC (including any personal email address) is strictly forbidden;
 - The user must be vigilant with regard to the identity of the authors of messages received, in particular from external correspondents, and take care not to open messages and attachments that appear to have an unknown or dubious origin;
 - Partial or total copying or reuse of all or part of CDC's and/or its clients' internal or external mailing lists is prohibited, except with CDC's express prior authorisation.
- In general, use of emails must comply with applicable regulations and RSSIPS requirements and, in particular, must not undermine the image, reputation, privacy or safety of others or of CDC and/or its clients, or the proper functioning of CDC's and/or its clients' resources.
- For security reasons, CDC may need to access messages received and sent in a user's electronic mailbox, without the user's authorisation and without their being present.
- Appropriate, responsible behaviour is the best protection against digital pollution, attacks aimed at abusing users (viruses, spam, phishing, spyware, hoaxes, etc.) and information leaks.
- *It is strictly forbidden to email any document belonging to CDC without the formal agreement of a CDC staff member. A CDC staff member must receive a copy of any CDC document sent externally.*

3.4

Uses of Internet services

- Although a major vector of infection, the Internet remains indispensable and requires even more precautions. At the same time, Internet services must not cause or be vectors of information leaks.
- As a matter of principle, Internet access is made available to users for the sole purpose of performing their services and within the limits of the rights granted and access authorised to Internet services by CDC.
- Only websites with a necessary direct link to the services for which the user is responsible may be consulted.
- As a preventive measure, CDC implements a number of website filtering systems, in particular targeting sites whose content may be contrary to public order or common decency.
- The user is informed of the risks associated with use of information exchange and communication services (forums, social networks and other collaborative services). As a result, the user is not authorised to use such collaborative services in ways not strictly necessary to their duties at CDC and not explicitly authorised by CDC (e.g. CDC's internal social network).
- *It is strictly forbidden to upload or share any document belonging to CDC using Internet services in the broadest sense, without the formal agreement of a CDC staff member.*

3.5

Use of telephony services (landline and mobile)

- Any telephones made available to users on an exceptional basis are strictly for the purpose of performing their services.
- Users are informed that the telephony system records outgoing telephone numbers. In addition, individual telephone records are drawn up every month; however, the last four digits of numbers are blacked out.
- Users are informed that, in principle, data relating to use of telephony services are only kept for a maximum period of one (1) year, in accordance with the legislation.

04

Intellectual property

- Respect for intellectual property, copyright and software license compliance is essential.
- Unless expressly authorised in advance by CDC, downloading and installation of software by the user is prohibited.
- Users are reminded that intellectual works such as software, photographs, images, databases, audiovisual and musical works, text files (studies, memos, consultations, analyses, notes of all kinds, diagrams, records and models), trademarks, designs, domain names and other distinctive signs, etc. are protected by intellectual property law.
- The user must therefore not use the resources in a way that infringes the CDC's, its clients' or third parties' intellectual property rights.
- *The user shall refrain from reproducing, depicting, publishing, exploiting and/or using any third-party files, data, software or databases protected by intellectual property or proprietary rights outside the legal or contractual possibilities granted to them.*

05

Protection of information and personal data

- All the organisational and technical measures taken to protect information, personal data in particular, will never replace human vigilance, which remains essential.
- The user has a general permanent obligation of confidentiality and discretion as regards the use of information, data and electronic documents available on CDC's and/or its clients' IS, in order to safeguard the assets and interests of CDC and/or its clients, as well as of the individuals concerned by such information, data or documents (partners, clients, suppliers, CDC staff, beneficiaries, etc.).
- The user shall take the utmost care to preserve the security (Availability, Integrity, Confidentiality and Proof) of the personal data to which they have access, in particular in order to ensure that CDC is able to comply with the provisions of European Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as well as Act no. 78-17 of 6 January 1978, amended, relating to information technology, data files and civil liberties, which requires that all necessary precautions be taken to preserve the security of said data and, in particular, prevent it from being distorted or damaged, or accessed by unauthorised third parties.

06

Controlling use of resources

- Control and monitoring measures are implemented in compliance with the principles of transparency and proportionality of means of collection, for the purposes of security, protection and verification of proper access to and use of resources.
- These measures are intended to:
 - guarantee the proper operation of resources,
 - monitor compliance with the rules governing use and security of CDC's and its clients' IS,
 - identify and, if appropriate, penalise uses that contravene applicable legislation and regulations,
 - ensure CDC is able to respond to requests from authorised public authorities (police, judicial authorities, etc.).
- The data and digital traces recorded as part of these measures concern identification of the user's account, the date and time of the action concerned, and its nature and results. These data and digital traces are kept for a maximum period of 18 months (unless there are specific legal or regulatory obligations to keep them for a longer period, e.g. limitation periods) and are subject to adequate protection measures against risks of disclosure and misuse.
- In addition, these data and digital traces are subject to automated processing for statistical purposes (number of messages sent to or received from the Internet, volumes occupied by all mailboxes, most-visited websites, frequency of access to the Internet or Intranet, number of pages visited, nature of pages visited, date, time and duration of connection, size of spaces on file servers, total duration of remote connections, etc.).
- When circumstances so require (events threatening the integrity and security of CDC's and/or its clients' IS), or when CDC's and/or its clients' responsibility or interests are at stake, all necessary means of investigation will be implemented by CDC, and if required, access to the resources of CDC's and/or its clients' IS may be restricted, or even closed, without prior notice.
- In the event of risk to CDC's and/or its clients' IS and/or inappropriate use of CDC's and/or its clients' resources, legal action may be taken against the user concerned, in particular on the basis of such connection data.

07

File servers

Confidential

22

Interne

Caisse des Dépôts

 |  |  |  [caissedesdepots.fr](https://www.caissedesdepots.fr)

Version 1 of 1 July 2021

- Content supplied in the context of performance of services must be stored and shared on the internal network's file servers, as instructed by CDC.
- Under no circumstances may users use these spaces or shared servers in general to store and/or share any files, documents or data (music, photos or videos in particular) unrelated to performance of services. Any content stored in breach of this prohibition may be deleted immediately and without prior notice to the user.

08

Information note: personal data

Confidential

24

Interne

Caisse des Dépôts

 |  |  |  [caissedesdepots.fr](https://www.caissedesdepots.fr)

Version 1 of 1 July 2021

- European Regulation (EU) 2016/679 of 27 April 2016 bearing on protection of individuals with regard to the processing of personal data and on the free movement of such data, together with Act no. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties, define the conditions under which personal data may be processed.
- Regulations governing protection of personal data prohibit collection and processing of data without the data subjects' knowledge, and also aim to preserve the confidentiality, security and integrity of personal data contained in data processing operations, which must comply with a specific legitimate purpose.
- In the context of these RSSIPS, personal data on users from CDC information systems and resources are processed at CDC, in particular in the context of the control systems provided for in the RSSIPS and in compliance with the aforementioned regulations. CDC undertakes to ensure that data concerning users are collected and processed fairly and lawfully, in accordance with the conditions described.
- As data controller, CDC pursues its legitimate interests and hence processes personal data relating to use of its information systems and resources covered by these RSSIPS and in order to ensure their security.
- More specifically, the data collected from users are required in order to provide them with the IT and communication resources they need to perform the services entrusted to them, and for the proper management, maintenance, organisation and security of information systems and resources.
- The data collected are kept for the entire duration of the commercial and contractual relationship, plus the duration of any legal requirements, with the exception of data and digital traces relating to resource usage controls, which are kept for a maximum period of 18 months (unless there are specific legal or regulatory obligations to keep such data for a longer period).
- Data concerning you may be transferred outside the European Union (to the United States), in the context of use of computer communication and electronic messaging tools published by Microsoft and made available to you at CDC. Such transfers are governed by standard contractual clauses drawn up by the European Commission.
- The data collected are intended for CDC's departments responsible for securing CDC's information systems or which are entitled to receive such data, on the basis of strict authorisations and restricted access, as well as, where applicable, its subcontractors and service providers mandated for the same purposes.

- Pursuant to the regulations in force, the user has the right to access, rectify and delete their data, limit their processing and object to their use, as well as the right to draw up directives on what is to happen to their data after their death, all of which can be exercised by email to mesdonneespersonnelles@caissedesdepots.fr or by post to the following address: Caisse des Dépôts et consignations – Données Personnelles - Établissement de Bordeaux – 5 rue du Vergne – 33059 BORDEAUX CEDEX – France
- For any further information or difficulties relating to the use of your data, you can contact our Data Protection Officer (DPO) at: dpo@caissedesdepots.fr
- In the event of any unresolved difficulty, you may refer the matter to the Commission Nationale de l'Informatique et des Libertés (CNIL – National Commission for Information Technology and Civil Liberties), the supervisory authority responsible for ensuring compliance with obligations relating to personal data.

Appendix

Model certificate of the service provider employee's compliance with CDC's information systems security rules.

I, the undersigned, [NAME, FIRST NAME, ADDRESS]

Acting on behalf of the service provider company [COMPANY NAME + Trade Register].

I hereby certify that I have been informed by the service provider of the CDC's information systems security rules for service providers (RSSIPS), that I have read them and that I undertake to comply with the obligations they contain.

Date

Signature.....